VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Tiina Mäkisalo

REKISTERÖIDYN OIKEUDET UUDISTUVASSA EUROOPAN UNIONIN TIETOSUOJA-ASETUKSESSA

Liiketalous

2017

VAASAN AMMATTIKORKEAKOULU

Liiketalous

TIIVISTELMÄ

Tekijä	Tiina Mäkisalo
Opinnäytetyön nimi	Rekisteröidyn oikeudet uudistuvassa Euroopan Unionin tietosuoja-asetuksessa
Vuosi	2017
Kieli	suomi
Sivumäärä	36
Ohjaaja	Marika Teirfolk-Naarmala

Opinnäytetyöni tavoitteena on selvittää lukijalle uudistuvan EU:n tietosuoja-asetuksen toteutumista käytännön tasolla. Uusi asetus (EU 2016/679) on yhteinen koko EU:n alueella ja sen käyttöönoton toivotaan yhtenäistävän EU-maiden tietosuojakäytäntöjä. Tällä hetkellä jokainen jäsenmaa on voinut toteuttaa voimassa olevaa asetusta parhaaksi katsomallaan tavalla. Tämä on johtanut hyvinkin kirjaviin lakeihin ja käytöntöihin eri maissa. Uusi tietosuoja-asetus korvaa Suomessa tällä hetkellä voimassa olevan henkilötietolain.

Vaikuttaa siltä että tietoturvauudistus on hyväksi niin asiakkaan tietoturvalle kuin yrityksillekin. Lakien yhtenäistäminen EU-alueella luo kansalaisille turvaa esimerkiksi eri maiden verkkopalvelujen käytössä koska vaatimukset ovat kaikille yrityksille samat. Yritykset myös varmasti hyötyvät muutoksesta kunhan myös ymmärtävät sen tuomat mahdollisuudet eivätkä koe muutosta vain pakkona.

Opinnäytetyössäni tutkin rekisteröidyn oikeuksia ja niiden muutoksia. Asetusta on noudatettava toukokuusta 2018 lähtien. Aiheesta voisi tehdä vielä myöhemmin jatkotutkimuksen jossa tarkasteltaisiin rekisteröityjen oikeuksien todellista toteutumista eri yrityksissä.

Avainsanat Tietosuoja, tietosuoja-asetus, rekisteröity

VAASAN AMMATTIKORKEAKOULU

UNIVERSITY OF APPLIED SCIENCES

Business Economics

ABSTRACT

Author	Tiina Mäkisalo
Title	The Rights of a Data Subject in the New EU General Data Protection Regulation
Year	2017
Language	Finnish
Pages	36
Name of Supervisor	Marika Terifolk-Naarmala

EU General Data Protection Regulation (GDPR) will affect all companies and organizations in the EU Countries from May 2018. The new Regulation (EU 2016/679) will be the same across the EU and its implementation is to be harmonized with the data protection practices in the EU. At present, each member state has been able to implement the existing regulation in the way it sees fit. This has led to different laws and practices in different countries. The new GDPR will replace the Personal Data Act currently in force in Finland.

I believe that the new regulation will be beneficial for both the customers and the businesses. Uniforming laws in the EU creates security for citizens. A good example is the use of online services in different countries because the requirements will now become the same for all companies across the EU. Hopefully companies will also see the positive sides and not just experience the change as a burden.

The aim of this Bachelor's thesis was to study the rights of the data subject. The regulation must be respected from May 2018. A further study on the realization of the rights for the data subjects in different companies could be carried out later.

Keywords GDPR, EU General Data Protection Regulation, data subject

SISÄLLYS

1 JOHDANTO

Tänä päivänä sähköiset henkilöstörekisterit ovat enemmänkin sääntö kuin poikkeus. Enää ei voida puhua kuinka digitalisoituminen on tulevaisuutta, koska se aika on tässä ja nyt. Tilastokeskuksen tekemän tutkimuksen mukaan internetiä käytti suomalaisista viime vuonna 88 prosenttia. Heistä 72 prosenttia vietti netissä aikaa useammin kuin kerran päivässä. Aika selvää onkin siis myös se, että alle 55-vuotiaiden kohdalla nämä molemmat luvut ovat lähes 100 prosenttia (Tilastokeskus 2017).

EU:n tietosuoja-asetus tuli voimaan 24.05.2016 ja sitä sovelletaan kaikissa jäsenmaissa 25.05.2018 alkaen. Uudistus korvaa kokonaan nykyisen henkilötietolain. Tällä hetkellä on siis parhaillaan menossa siirtymäaika, jonka jälkeen henkilötietojen käsittelyn on oltava uuden asetuksen mukaista. Aihe on mielestäni erittäin ajankohtainen, koska henkilötietoja käsitellään nykyään aina vain suuremmissa määrin esimerkiksi erilaisissa verkkokaupoissa. Tietojen säilyttäminen erilaisissa tietojärjestelmissä ja verkossa altistaa tiedot myös uusille ja erilaisille riskeille.

Tietosuojavaltuutetun toimisto teki kesällä 2012 kyselyn 74 yritykseen ja yhteisöön. Kyselyyn valittiin sellaiset toimijat joihin oli kohdistunut tietoturvaloukkaus tai sen uhka lokakuu-joulukuu 2011 välisenä aikana. Tarkoituksena oli selvittää miten tietoturvauhkiin oli varauduttu, miten loukkaukset selvisivät ja ilmoitettiinko niistä henkilöille joiden tiedot olivat kyseessä. Samalla tutkittiin myös kuinka hyvin henkilötietolaki tunnetaan kyseisissä yrityksissä ja yhteisöissä. Selvisi että yrityksistä 30% ei ollut tehnyt minkäänlaisia toimenpiteitä tietoturvaloukkauksen tai sen uhan jälkeen. Vain 46% vastanneista kertoi tuntevansa henkilötietolain vaatimukset. (Tietosuojavaltuutetun toimisto, 2012) Huolestuttavan suuri osa yrityksistä ei siis tunne lain vaatimuksia henkilötietojen säilyttämisen ja käsittelyn osalta. On hieman huolestuttavaa että kenen tahansa tiedot saattavat joutua ulkopuolisten käsiin eikä asianomaiselle henkilölle ilmoiteta mitään. Oman vaaransa asiaan tuo

myös se seikka, että todennäköisesti kaikki yritykset eivät edes tunnista heihin kohdistunutta uhkaa.

Tietosuojan ja ihmisten yksityisyyden suojaamisen tarve on siis muuttunut paljonkin vuosien saatossa jolloin myös lainsäädäntöä tulee aika ajoin täsmentää. Rekisterinpitäjät niin yksityisellä kuin julkisellakin sektorilla ovat tällä hetkellä kovan paineen alla saadakseen henkilötietojen käsittelyyn tarkoitetut järjestelmät ajan tasalle ennen toukokuuta 2018.

1.1 Tutkimus ja sen tavoite

Tässä Oikeustradenomin lopputyössäni käsittelen Euroopan Unionin tietosuojauudistusta. Aikaisempaa tietosuojalainsäädäntöä on EU:n alueella toteutettu hyvinkin erilaisilla tavoilla jäsenvaltiosta riippuen (Vanto, 2011, 16). Lakiuudistuksen tavoitteena onkin nyt yhtenäistää EU-alueen lainsäädäntö jolloin henkilötietojen käsittelyä toteutettaisiin samalla tavoin jokaisessa jäsenmaassa. Myös Suomessa tulee käydä läpi koko lainsäädäntö, koska kansallinen lainsäädäntö ei voi olla ristiriidassa EU lainsäädännön kanssa (Andreasson, Koivisto, Ylipartanen 2014, 18).

Etsiessäni tietoa aiheesta ja lukiessani siitä löytyvää kirjallisuutta päätin tarkastella uudistuvaa lainsäädäntöä ja sen tuomia muutoksia erityisesti rekisteröidyn henkilön kannalta. Vaikka uudistus tuo enemmän työtä ja muutoksia rekisterinpitäjille, on myös rekisteröidyn asema mielenkiintoinen. Rekisterinpitäjille on myös olemassa monia eri ohjeita lakimuutokseen varautumisesta, rekisteröidylle ei mitään. Työn tarkoitus on siis tarkemmin selvittää mitä rekisteröidyn oikeudet ovat, miten ne muuttuvat lakimuutoksen myötä ja miten oikeuksia tulisi käytännössä soveltaa. Mitä esimerkiksi tietojen tarkistusoikeus käytännössä tarkoittaa? Miten toimia jos haluaa tarkistaa tietonsa jostain rekisteristä?

2 UUDISTUVAN TIETOSUOJALAIN TAUSTAT JA TAVOITTEET

Tietosuojalain taustalla on luonnollisesti ajatus suojata ihmisen yksityiselämää. Siihen on yhdistetty ihmisen oikeus määrätä kuka, missä ja miten hänen henkilötietojaan käsitellään. Henkilösuojan tarpeeseen on johtanut esimerkiksi toisen maailmansodan tapahtumat Hollannissa. Tuolloin ihmisiä rekisteröitiin reikäkorteille, jotta heidän voitiin myöhemmin luokitella uskonnon mukaan. Juutalaiset saatettiin näin lähettää keskitysleirille (Neuvonen, 2014, 59). Tänä päivänä ihmisten rekisteröinti uskonnon mukaan on laissa kielletty.

Yksityisyys on aina ollut ihmisille tärkeää, jo paljon ennen kuin henkilötietosuojasta säädettiin lailla. Jo antiikin Roomassa asiat oli jaoteltu publicusiin ja privatusiin. Julkinen toiminta oli valtion toimintaa ja kaikki muu toiminta oli yksityistä. (Neuvonen, 2014, 21). Monia asia on kuitenkin vuosikymmenien ja -satojen saatossa muuttunut ja lakeihin on tehty paljon muutoksia. Euroopassa tärkeimpiin tapahtumiin nykyisen lain saavuttamiseksi voidaan lukea Euroopan neuvoston ministerikomitean lausumia vuosilta 1973 ja 1974. Nämä lausumat sisälsivät pääperiaatteet henkilötietojen suojasta. Tämän jälkeen vuonna 1980 Taloudellisen yhteistyön ja kehityksen järjestön (OECD) antamat ohjeet henkilötietosuojasta ja tietojen siirtämisestä vastaavat terminologialtaan jo lähes täysin nykyistä asetusta. Ohjeistuksessa pääkohtia ovat tietojen keruun rajoitus, tietojen laatu, käyttötarkoitussidonnaisuus, henkilötietojen käytön rajoitus, tietoturvallisuus, avoimuus sekä yksilön oikeudet. (Vanto, 2011, 13) Voidaankin siis todeta henkilötietosuojan perusperiaatteiden säilyvän edelleen lähes muuttumattomina vaikka yhteiskunta on läpikäynyt suuria muutoksia vuosikymmenten saatossa varsinkin internetin valtakauden alkaessa 1990-luvun puolivälin jälkeen.

Seuraava askel kohti nykyistä lainsäädäntöä on Euroopan neuvoston yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä vuodelta 1981. Sopimus sisältää neljä henkilötietojen suojan periaatetta joita ovat; tietojen laatu, erityiset tietoryhmät, tietoturva sekä lisätoimet rekisteröidyn suojelemiseksi.

Yleissopimuksen jälkeen monet Euroopan maat säätivät oman henkilötietolakinsa. Suomessa ensimmäinen henkilötietoihin kohdistuva laki oli henkilörekisterilaki (HRL 471/1987). Lait poikkesivat kuitenkin monelta osin toisistaan ja vuosien mittaan on käynyt aina vain selvemmäksi, että EU jäsenmaiden välille tarvitaan yhteinen henkilötietosuojalaki.

EU:n tietosuojadirektiiviksi kutsutaan 24.10.1995 annettua *Euroopan parlamentin ja neuvoston direktiiviä 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta*. Kansalliset lakimuutokset tuli toteuttaa kolmen vuoden sisällä. Suomi siis myöhästyi tuolloin aikataulusta, koska henkilötietolaki tuli voimaan vasta 1999. EU:n tietosuojadirektiivi ja Suomen henkilötietolaki ovat voimassa siihen asti kunnes uusi tietosuoja-asetus otetaan lopullisesti käyttöön 28. toukokuuta 2018.

Euroopan unionin tietosuojadirektiivi vuodelta 1995 ohjasi jäsenmaita yhtenäisempään lainsäädäntöön. Suomessa henkilörekisterilaki vuodelta 1987 korvattiin henkilötietolailla vuonna 1999 (HeTiL 523/1999). Kuitenkin vielä tietosuojadirektiivin antamisenkin jälkeen jäsenmaiden lait poikkesivat suuresti toisistaan. Joissain maissa henkilötietojen siirtäminen maasta toiseen oli laitonta, kun taas toisaalla se saattoi olla laillista, mutta vain erittäin byrokraattista (Vanto, 2011, 16).

Henkilötietoja suojataan myös rikosoikeudellisesti. Rikoslain 24 luku kriminalisoi muun muassa kunnianloukkauksen ja yksityiselämää loukkaavaan tiedon levittämisen. Rikoslaki luku 38 säätää myös viestintäsalaisuuden loukkauksesta, tietomurrosta ja henkilörekisteririkoksesta. (RL 24:1-9, 38:1-2) Rikoslaki rankaisee tehdyistä virheistä jälkikäteen kun taas säädöksillä henkilörekistereistä pyritään ennaltaehkäisemään väärinkäytöksiä. Myös ihmisten sosiaalinen kanssakäyminen ja käytös vaikuttaa paljon siihen miten toimimme.

Nyt annettu henkilötietodirektiivi velvoittaa jäsenmaat säätämään lakinsa saman arvoisiksi jotta jokaisella kansalaisella olisi yhtäläiset oikeudet hänen henkilötietojaan käsitellessä. Nähtäväksi kuitenkin jää miten jäsenmaat asetusta todella toteuttavat. Erittäin mielenkiintoinen on myös kysymys siitä milloin tulee

seuraavan kerran tarve tarkentaa, muuttaa tai lisätä jotain nyt voimaan astuvaan tietosuoja-asetukseen.

2.1 Tietosuojan tarve ja tarkoitus

Henkilötietosuojasta ja tietosuojasta puhutaan toistensa synonyymeinä. Näiden kahden käsitteen ero on siinä, että henkilötietojen suoja on oikeudellinen peruskäsite. Oikeuslingvistisesti ja lakiteknisesti katsotaan että henkilötietojen suoja on tietosuojalainsäädännön avulla toteutettua yksityisyyden suojaa ja siten sillä suojataan yksilön perusoikeutta. Tietosuojallakaan ei kuitenkaan aina tarkoiteta pelkän tiedon suojaamista vaan myös sillä on usein tarkoitus suojata henkilön tietoja ja oikeuksia. Tietosuojasta onkin siis tullut vakiintunut käsite henkilötietojen suojaamisesta puhuttaessa. Myös valvovaa viranomaista kutsutaan lyhyesti tietosuojavaltuutetuksi. Tietosuojaa laajempi käsite taas on tietoturva jolla tarkoitetaan kaiken tiedon, esimerkiksi liikesalaisuuksien suojaamista ulkopuolisilta. (Saarenpää 2012, 318-319)

Tietosuojan tarve ilmenee monella tapaa. Ensisijaisesti sillä pyritään suojaamaan yksityishenkilön tietoja ulkopuolisilta. Toisaalta sillä on iso merkitys myös yrityksille jotka pitävät henkilörekistereitä ja keräävät asiakkaistaan tietoja. Olisi suuri kolhu yrityksen maineelle, mikäli tieto asiakkaista leviäisi yrityksen ulkopuolelle. Luottamus yritykseen ei olisi enää samalla tasolla jos yrityksen havaittaisiin käyttävän henkilötietoja väärin tai suojaavan niitä huonosti jolloin ulkopuolinen saattaisi päästä niihin käsiksi. Tästä saattaisi koitua maineen menettämisen lisäksi myös taloudellisestikin suuret tappiot.

Tietosuojasta säätämällä pyritään toteuttamaan henkilöiden tasapuolinen kohtelu heidän yksityistietojensa suojaamisessa. Henkilötietolainsäädännön yksi keskeisistä periaatteista on että henkilötietojen käsittelyn on perustuttava henkilön suostumukseen. Nykyisen voimassa olevan lain tavoitteena on siksi myös hallituksen esityksen mukaan ollut osoittaa milloin henkilön tietojen käsittely voidaan toteuttaa ilman henkilön myötävaikutusta. Lain muita tavoitteita ovat esimerkiksi hyvän tietojenkäsittelyn kehittäminen ja noudattaminen sekä yhtenäisen tietojenkäsittelytavan toteuttaminen (HE 96/1998, 30).

2.2 Euroopan parlamentin henkilötietoasetus

Tietosuojadirektiivin lisäksi on säädetty henkilötietoasetus nimeltään *Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001 yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta*. Tämä asetus koskee kaikkia Euroopan parlamentin käsittelemiä henkilötietoja. Asetuksella pyritään suojelemaan luonnollisten henkilöiden perusvapauksia ja perusoikeuksia heitä koskevien henkilötietojen käsittelyssä. (European Parliament, 2001)

Oikeus henkilötietojen suojaan on vahvistettu EU:n perusoikeudeksi Lissabonin sopimuksella joulukuussa 2007 (Neuvonen, 2014, 55). Tietosuojan vahvistaminen perusoikeudeksi kertoo paljon tekniikan hurjasta kehityksestä, koska EU:n perustamiskirjan muista oikeuksia ovat muun muassa oikeus vapauteen ja turvallisuuteen sekä oikeus elämään ja orjuuden ja pakkotyön kielto. (Euroopan unionin perusoikeuskirja, 2000, 2-5 artikla). Näiden rinnalla henkilötietojen käytön valvominen teknisessä mielessä tuntuu mitättömältä. Tosiasia kuitenkin on, että henkilötietoja käsitellään jatkuvasti ja ilman niitä on vaikeaa tehdä esimerkiksi sähköistä kauppaa. Digiaikana vaara henkilötietojen leviämisestä tai niiden hakkeroinnista on myös paljon suurempi kuin aikaisemmin.

Direktiivi on ohjeistus jonka pohjalta kukin jäsenmaa saa soveltaa omaa kansallista lainsäädäntöään. Nykyisen direktiivin tilalle annetaan asetus. Asetus on pakottavaa lainsäädäntöä joka on otettava kaikissa jäsenmaissa käyttöön sellaisenaan. (Ruonala, 2011, 172)

2.3 Tietosuojadirektiivi sähköisestä viestinnästä

Euroopan parlamentti ja neuvosto on 7.2.2002 antanut direktiivin 2002/21/EY, sähköisten viestintäverkkojen- ja palvelujen yhteisestä sääntelyjärjestelmästä. Siinä on sovittu pelisäännöt televiestintämarkkinoiden kilpailun avaamiselle EU:n alueella. Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi) on osa televiestintäpakettia johon

sisältyy neljä erityisdirektiiviä ja kaksi asetusta (Sähköisen viestinnän sääntelyjärjestelmä, 2002, 1). Sähköisen viestinnän tietosuojadirektiivillä pyrittiin yhdenmukaistamaan jäsenvaltioiden lainsäädäntöä sähköisen viestinnän alalla. Direktiivi 2002/58/EY ohjeistaa niin sähköpostilla tehtävän suoramarkkinoinnin toteuttamisessa kuin sijaintitietojen käsittelyssä.

Sähköisen viestinnän tietosuojadirektiivi otettiin suomessa käyttöön säätämällä Sähköisen viestinnän tietosuojalaki 516/2004. Laki on sittemmin kumottu Tietoyhteiskuntakaarella 917/2014. Tietoyhteiskuntakaareen on sisällytetty sähköisen viestinnän tietosuojalain lisäksi seitsemän eri lakia kuten Televisio- ja radiotoimintalaki sekä Viestintämarkkinalaki. Näistä on pyritty saamaan kattava kokonaisuus muuttuvaa tietoyhteiskuntaa varten.

Nykyaikana tieto ja laki on monesti vanhaa jo julkaisupäivänään. Lakien säätäminen kestää usein vuosikausia ja siitä syystä aika on usein ajanut lain ohi ennen sen valmistumista. Nimen omaan tästä syystä Tietosuojauudistuksenkin jalanjäljissä on jo tehty uusi esitys myös sähköisen viestinnän lainsäädännön päivittämisestä. Euroopan komission on julkistanut uuden ehdotuksen tammikuun 10. päivä 2017. Ehdotuksella pyritään uusien mahdollisuuksien luomiseen tietojenkäsittelyssä. Evästeiden käytön säätelyä kevennettäisiin kun taas esimerkiksi mainospostin ja myyntipuheluiden vaatimuksia kiristettäisiin. Keskeisiin tavoitteisiin kuuluu myös digitaalisten sisämarkkinoiden luottamuksen lujittaminen ja turvallisuuden parantaminen. Uusi säädös sitouttaisi mukaan perinteisten teleoperaattoreiden lisäksi sähköisten viestintäpalveluiden uudet tulokkaat kuten Facebook Messenger, WhatsApp, iMessage ja Skype.

Uusi laki kattaisi myös tietosuojauudistuksen tapaan kaikki jäsenmaat. Tarkoitus on myös helpottaa eri maissa toimivien yritysten asemaa. Nykyisen lainasäädännön alla kansainväliset yritykset joutuvat noudattamaan EU:n sisälläkin maiden kirjavaa lainsäädäntöä. Jäsenmaiden lainsäädännön yhtenäistäminen helpottaisi monen yrityksen toimia. Uutta asetusta myös tiukennettaisiin niin että se olisi henkilötietojen suojauksen osalta samassa linjassa Tietosuojauudistuksen kanssa. (Euroopan komissio, 2017)

2.4 Tietosuojan toteuttaminen käytännössä

Tietosuojaa voi parantaa ja ylläpitää monin eri tavoin. Sen huolellinen suunnitteleminen ja toteuttaminen myös käytännön tasolla on erittäin tärkeää. Vaikka yrityksellä olisi käytössään turvalliset järjestelmät, käyttävät tietoja kuitenkin pääasiassa ihmiset. Virheiden välttämiseksi työntekijät eli henkilötietojen käsittelijät onkin syytä perehdyttää tehtäviinsä hyvin.

Jokaisen henkilötietojen käsittelijän tulee huolehtia niin omasta toiminnastaan kuin koko yrityksen tietoturvasta. Yksinkertaisimmillaan tietoturva on ovien lukitsemista ja salasanojen tallessa pitämistä. Tulee huolehtia että niihin tiloihin jossa henkilörekisteriä ylläpidetään tai säilytetään on pääsy vain siihen valtuutetuilla henkilöillä. Tähän kuuluvat kiinteästi kulkulupien ja avaimien huolellinen säilyttäminen. Myös asiakirjojen säilyttäminen niille kuuluvassa paikassa on tietoturvaa yksinkertaisimmillaan.

Työntekijöiden käyttöoikeuksien rajaamisella voidaan selkeyttää tietoihin pääsyä ja jakaa käyttäjät helposti ryhmiin. On tärkeää roolittaa käyttäjät jolloin on helppoa jakaa tarvittavat käyttöoikeudet niitä tarvitseville, mutta estää pääsy siihen osaan tiedosta jota ei työtehtävien suorittamiseen tarvita. Käyttäjäryhmien valvominen on helpompaa, eikä työntekijä voi myöskään vahingossa koskea hänelle kuulumattomiin tietoihin. Työsuhteen alussa on syytä selvittää työntekijälle myös onko hänen allekirjoitettava salassapitosopimus. Myös käsitteet vaitiolovelvollisuus ja asiakirjasalaisuus on hyvä käydä yhdessä läpi.

Nykyisin suuria tietoturvariskejä saattavat muodostaa myös etätyö ja järjestelmien etäkäyttö. Palomuurien ja virustorjunnan tulee olla kunnossa. Yhteyksien tulisi olla salattuja ja suojatuttuja. Sähköpostin käytössä tulee miettiä millaiset viestit vaativat lähettämisen olevan salattua. Jokaisen yrityksen olisi myös syytä tehdä sosiaalista mediaa koskevat ohjeet henkilökunnalle jotta työntekijät eivät puhuisi työpaikan asioista vapaa-ajallaan. (Andreasson ym. 2013, 44-61)

3 SUOMEN NYKYINEN TIETOSUOJALAINSÄÄDÄNTÖ

Tietoyhteiskuntakaari otettiin käyttöön tammikuun ensimmäinen päivä vuonna 2015. Lain toteuttaminen vaati pitkäjänteistä työtä. Tietoyhteiskuntakaaren suunnittelu aloitettiinkin jo joulukuussa 2011 ja hankkeen läpiviemiseen käytettiin kolme vuotta. Säädöksiä yhtenäistettiin niin, että noin 490 pykälää saatiin tiivistettyä runsaaseen 350 pykälään. Tietoyhteiskuntakaarella pyrittiin parantamaan sähköisen viestinnän osalta kuluttajansuojaa, tietoturvaa ja yksityisyyden suojaa. Edellä mainitut vaatimukset laajennettiin koskemaan kaikkia viestinnän harjoittajia. (Bergström, 2014) Todennäköistä kuitenkin on, että myös Tietoyhteiskuntakaarta joudutaan monilta osin vielä tarkentamaan kun maailma muuttuu ja digitalisoituu jatkuvasti.

Tietoyhteiskuntakaaren lisäksi Suomessa noudatetaan henkilötietosuojan osalta kuitenkin suurimmaksi osaksi Henkilötietolain (523/1999) säädöksiä. Nykyinen lainsäädäntö on voimassa vielä siirtymäajan loppuun toukokuuhun 2018. Alla tarkemmin Henkilötietolain sisällöstä.

3.1 Henkilötietolain tarkoitus ja soveltamisala

Henkilötietolain 523/1999 mukaan sen tarkoituksena on "toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista". Henkilötietolakia sovelletaan kun henkilötietoja käsitellään automaattisesti ja muuhun henkilötietojen käsittelyyn silloin kun tiedot muodostavat tai niiden on tarkoitus muodostaa osa tai kokonainen henkilörekisteri. Henkilötietojen käsittely ei siis aina edellytä tietotekniikkaa vaan ehdot täyttää jo esimerkiksi seuran tai yhdistyksen ruutupaperille keräämä nimi- tai osoitelista. Henkilötietolain säädökset eivät koske yksityishenkilöiden omaan käyttöön ylläpitämiä puhelin- tai osoitetietoja. Näin esimerkiksi matkapuhelimessa säilytettävät yhteystiedot eivät muodosta laissa tarkoitettua henkilötietorekisteriä. Yleisellä tasolla kannattaa kuitenkin huolehtia myös niiden hyvästä säilyttämisestä.

Henkilötietolaki on henkilötietoja säätelyä koskeva yleislaki. Henkilötietolaki on myös toissijainen; mikäli henkilötietojen käsittelystä on säädetty jossain toisessa laissa, menevät erityislait henkilötietolain edelle. Henkilötietolailla voidaan myös täydentää erityislakeja. (Pitkänen,Tiilikka &Warma, 2013, 30)

3.2 Henkilötietojen käsittelyä koskevat määritelmät ja periaatteet

Jotta lakia osattaisiin tulkita sen vaatimalla tavalla, on tärkeää ymmärtää sitä koskevat määritelmät ja käsitteet. Henkilötietolaki 523/1999 pykälä 3 antaa seuraavat määritelmät:

a) henkilötieto; henkilötiedoiksi luetaan kaikki sellaiset tiedot joilla voidaan tunnistaa henkilö tai hänen perheensä tai muu samassa taloudessa elävä henkilö. Tiedot voivat olla tavanomaisen nimen ja henkilötunnuksen lisäksi myös mitä tahansa muista tietoja joista henkilö tai hänen läheisensä ovat tunnistettavissa.

b) henkilötietojen käsittely; kaikki henkilötietoihin kohdistuvat toimenpiteet niiden keräämisestä poistamiseen asti.

c) henkilörekisteri; rekisteri muodostuu automaattisesti tai manuaalisesti käsitellystä henkilötietojen joukosta joka on järjestetty niin, että tiettyä henkilöä koskevat tiedot voidaan löytää rekisteristä helposti.

d) rekisterinpitäjä; taho jonka käyttöön rekisteri perustetaan ja joka määrää sen käytöstä. Rekisterinpito voi olla myös laissa tällaiselle henkilölle/henkilöille, säätiölle, laitokselle tai yhteisölle määrätty.

e) rekisteröity; se henkilö jonka tietoja rekisterissä käsitellään.

f) sivullinen; muu henkilö tai taho kuin kaksi yllä mainittua.

g) suostumus; suostumuksella tarkoitetaan kaikenlaista tahdon ilmaisua jolla rekisteröity henkilö hyväksyy sen että hänen henkilötietojaan käsitellään kyseessä olevassa henkilötietorekisterissä. Tahdon ilmaisun tulee olla vapaaehtoinen, yksilöity ja tietoisesti tehty.

Henkilötietojen käsittelylle tulee aina olla laissa säädetty oikeusperuste (Vanto, 2011, 14). Henkilötietorekisteriin ei saa tallettaa tietoja jotka koskevat henkilön seksuaalista suuntautumista tai käyttäytymistä, rotua tai etnistä alkuperää, yhteiskunnallista, poliittista tai uskonnollista vakaumusta. Myöskään ammattiliittoon kuulumista ei saa rekisteröidä. Muita arkaluontoisia tietoja ja siten niiden kiellettyä käsittelyä ovat rikokset ja rangaistukset sekä terveydentilaa, sairautta tai vammaisuutta sekä niiden hoitoa koskevat tiedot. (Henkilötietolaki 523/1999 §11) Samat periaatteet koskevat myös uuttaa tietosuoja-asetusta.

3.3 Muu henkilötietoja koskeva lainsäädäntö

Henkilötietolain lisäksi on olemassa useita erikoislakeja henkilötietojen käsittelyä koskien. Yleisimmin henkilötietoja käsitellään esimerkiksi työpaikoilla henkilöstöhallinnossa, sairaanhoidossa sekä poliisiasioissa. Muutamina esimerkkeinä laeista joissa säädetään henkilötietojen käsittelystä voisi mainita Laki henkilötietojen käsittelystä poliisitoimessa (761/2003/), laki henkilötietojen käsittelystä rajavartiolaitoksessa (579/2005) sekä laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007).

Muiksi varsinaisesti tietosuojaa koskeviksi laeiksi voidaan laskea myös laki yksityisyyden suojasta työelämässä (759/2004) sekä laki sähköisen viestinnän tietosuojasta (516/2004). Lakeja sovelletaan soveltamisalueidensa mukaisesti ensisijaisina ja täydentävästi henkilötietolakiin nähden. Mikäli viranomaisten henkilörekisteristä luovutetaan tietoja, tulee sovellettavaksi myös viranomaisten toiminnan julkisuudesta annettu laki (621/1999).

4 EUROOPAN UNIONIN UUDISTUVA TIETOSUOJALAINSÄÄDÄNTÖ

Tietosuoja-asetuksen säätäminen aloitettiin vuoden 2012 alussa, jolloin se hyväksyttiin Euroopan komissiossa ja lähettiin eteenpäin lausuntokierrokselle. Neljän vuoden työskentelyn jälkeen tarjolla on uusi koko EU:n kattava lainsäädäntö jota jokaisen täällä toimivan yrityksen ja yhteisön on noudatettava. Uudistuvan tietosuojalain keskeisimmät muutokset pyrkivät edistämään avoimuutta ja läpinäkyvyyttä henkilötietojen käsittelyssä. Tavoitteena on myös vahvistaa ja selkeyttää rekisteröityjen oikeuksia. Asetus tuo rekisterinpitäjille ankarammat velvollisuudet kuin aikaisemmin asettaen myös ankarammat seuraukset rikkomuksista. Uusi lainsäädäntö asettaa velvollisuuksia myös suoraan henkilötietojen käsittelijälle.

Nyt jos koskaan olisi yritysten hyvä aika tehdä paljon puhuttu tietotilinpäätös. Tietotilinpäätöksellä tarkoitetaan raporttia jolla kuvataan tietosuojan nykytilaa yrityksessä. Siitä pitäisi selvitä ainakin miten tietosuojaa ja -turvaa toteutetaan kyseisessä organisaatiossa ja miten tietoturvaan liittyvää riskinhallintaa harjoitetaan. Hyvin toteutettu tietotilinpäätös myös ohjaa toiminnan suunnittelussa ja raportoinnissa. Se antaa kattavan kuvan kehityskohteista ja sen avulla voidaan seurata niiden toteutumista. Suuressa organisaatiossa se myös esittelee eri osastojen vastuut. Hyvin laadittu dokumentti herättää luottamusta niin organisaation sisällä kuin sen sidosryhmissäkin. Tietotilinpäätös ei ole lakisääteinen, mutta Tietosuojavaltuutettu suosittelee sen tekemistä. (Andreasson ym. 2014, 118-120)

4.1 Määritelmät ja periaatteet

Tietosuoja-asetuksen tavoitteena on suojella luonnollisten henkilöiden oikeutta henkilötietojen suojaan. Asetuksella pyritään myös turvaamaan henkilötietojen vapaa liikkuvuus unionin rajojen sisäpuolella sekä tietysti suojaamaan rekisteröityjen perusoikeuksia ja -vapauksia. Uutta asetusta sovelletaan kaikkeen automaattiseen, osittain automaattiseen tai manuaaliseen henkilötietojen käsittelyyn joiden on tarkoitus muodostaa henkilörekisteri tai sen osa.

Asetuksen määritelmät Artiklassa 4 ovat osittain samat kuin jo yllä mainitussa henkilötietolaissa. Niitä on monilta osin tarkennettu joka osaltaan auttaa lain soveltamisessa. Nostaisin esiin seuraavat määritelmät joita nykyinen lainsäädäntö ei tunne:

- profilointi: käsitteellä tarkoitetaan henkilötietojen automaattista käsittelyä jonka avulla voidaan analysoida tai ennakoida piirteitä jotka liittyvät esimerkiksi henkilön kiinnostuksen kohteisiin, terveyteen, työsuorituksiin tai vaikka käyttäytymiseen. (Tietosuoja-asetus 679/2016, artikla 4)

- pseudonymisointi: tietoja käsitellään niin että yksittäistä henkilöä ei voida niistä enää tunnistaa (Tietosuoja-asetus 679/2016, artikla 4)

Myös asetuksen periaatteet säilyvät pääosin samoina kuin aikaisemminkin. Henkilötiedot saa kerätä ainoastaan ennalta määriteltyä tarkoitusta varten (käyttötarkoitussidonnaisuus). Niitä saa kerätä vain sen verran kuin oikeasti on tarvetta. Erityisiä henkilötietotyhmiä ei muutamaa poikkeusta lukuun ottamatta saa edelleenkään käsitellä. Näitä tietoja ovat mm. rotu, uskonnollinen vakaumus, ammattiliiton jäsenyys tai geneettiset ja biometriset tiedot. Rekisterinpitäjän tulee myös varmistua siitä, että tiedot ovat oikeita ja luotettavia. Niitä on käsiteltävä niin lainmukaisesti, asianmukaisesti kuin rekisteröidyn kannalta läpinäkyvästikin. Tietojen on oltava ajantasaisia ja virheettömiä, epätarkat tai virheelliset tiedot tulee viipymättä poistaa tai oikaista. Henkilötiedot tulee säilyttää turvallisesti asiattomien ulottumattomissa ja vain sen ajan kuin on tarpeellista. (Tietosuoja-asetus 679/2016, artikla 5)

4.2 Lainmukaisuus ja suostumuksen ilmaiseminen

Henkilötietojen käsittely lainmukaisuusperiaate täyttyy silloin kun rekisteröity on antanut tietojensa käyttöön nimenomaisen ja yksilöidyn suostumuksen. Tahdon ilmaisun täytyy olla selvä ja yksiselitteinen. Rekisterinpitäjän tulee myös pystyä osoittamaan että rekisteröity on antanut suostumuksensa rekisteröintiin. Useiden verkkopalveluiden käyttöehdot on tähän asti voinut hyväksyä valmiiksi rastitetun ruudun ohittamalla. Uuden asetuksen voimaantulon jälkeen sitä ei lueta enää

suostumukseksi, vaan palveluntuottajan on pystyttävä osoittamaan että rekisteröity on itse aktiivisesti laittanut rastin ruutuun hyväksyäkseen ehdot.

Asetuksessa määrätään erikseen että alle 16-vuotiaan lapsen kohdalla myös vanhemman on annettava suostumuksensa lapsen henkilötietojen käsittelyyn. Jäsenmaat saavat omilla asetuksillaan määrätä kansallisella tasolla ikärajan 13-16-vuoden välille. Käytännössä monen sosiaalisen median palvelun ikäraja on nyt asetettu 13 ikävuoteen. Tarkastellessa eri palveluiden verkkosivuilta löytyviä yleisiä ehtoja selviää että näin toimivat ainakin Facebook, Twitter ja WhatsApp. WhatsAppin yleiset ehdot mainitsevat vielä erikseen että ikäraja saattaa myös olla korkeampi kansallinen lainsäädäntö huomioon ottaen. Näistä kolmesta vain WhatsAppissa alaikäisen vanhemmat voivat antaa lapselle luvan palvelun käyttöön (WhatsApp 2016).

Lainmukaisuus rekisteröityjen tietojen käyttöön täyttyy myös jos tietojen käsittely on edellytyksenä esimerkiksi sopimuksen tekemiseksi. Tällöin rekisteröinti on tehtävä jotta rekisterinpitäjän lakisääteinen velvollisuus saadaan täytettyä tai käsittelyllä suojataan rekisteröidyn tai jonkun toisen elintärkeitä etuja. Laillista on myös rekisteröidä henkilö silloin kun sitä vaaditaan rekisterinpitäjän tai kolmannen osapuolen etuoikeutettujen etujen toteuttamiseksi, julkisen vallan käyttämisen tai yleistä etua koskevan tehtävän suorittamiseksi. Jotta henkilötietojen lainmukaisessa rekisteröimisessä voitaisiin viitata kahteen viimeiseen kohtaan (julkinen valta ja yleinen etu), on niistä oltava erikseen kohdat kansallisessa lainsäädännössä.

EU-maiden tietosuojavaltuutetuilla on yhteinen elin nimeltään WP (working party) 29. WP29 valmistelee tällä hetkellä tarkempaa tietosuoja-asetukseen liittyvää ohjeistusta. Julkaisuilla tulee varmasti jatkossa olemaan tärkeä merkitys sen suhteen, miten tietosuoja-asetusta pitäisi tulkita. Jo aiemmin julkaistuja ohjeita on kolme; oikeudesta tiedon siirtoon (Data portability), tietosuojavastaavista (Data Protection Officers DPO) sekä siitä miten johtava valvontaviranomainen määrätään (Lead Supervisory Authority). (European Comission 2016)

4.3 Riskitason arviointi

Tietosuoja-asetus on velvoitteiden määräytymisen osalta riskiperusteinen. Se tarkoittaa että rekisterinpitäjä on velvollinen arvioimaan henkilörekisterinsä laajuuden, luonteen ja riskit. Arvion pohjalta on pystyttävä suunnittelemaan ja toteuttamaan tarvittavat toimenpiteet riskien minimoimiseksi sekä niiden hallitsemiseksi. Arvio ja suunnitelma on tehtävä aina ennen rekisterin käyttöönottoa. Tätä kutsutaan tietosuojaa koskevaksi vaikutustenarvioinniksi. Vaikutustenarviointi on pakollinen niille yrityksille joiden henkilötietorekistereissä on suurimmat riskit. Tällaisia ovat ainakin yritykset jotka käsittelevät henkilötietorekistereitä tehden päätöksiä automaattisesti. Myös sellaiset tahot jotka käsittelevät rikostuomioita tai muita rikkomuksia tai erityisiä henkilötietoryhmiä kuuluvat korkean riskin ryhmään. (Tietosuoja-asetus 679/2016, Artikla 35)

Vaikutustenarviointi kuitenkin suositellaan kaikkien tehtäväksi. Artikla 35 määrää vaikutuksenarvioinnin keskeisen sisällön. Jos riski rekisteröidyn oikeuksien ja vapauksien kannalta luokitellaan suureksi eikä rekisterinpitäjä pysty pienentämään riskiä omin voimin, tulee hänen olla yhteydessä tietosuojavaltuutettuun ennakkokuulemista varten. Tietosuojavaltuutettu on myös velvollinen julkaisemaan listan josta selviää tarkemmat ohjeet siitä, millaiset rekisterit ja käsittelytoimet vaativat tarkempaa vaikutustenarviointia. Vaikutustenarviointi edistää myös osoitusvelvollisuuden toteutumista ja näin edesauttaa rekisterinpitäjän velvollisuuksien toteutumista. (Tietosuoja-asetus 679/2016, Artikla 35).

4.4 Rekisterinpitäjän yleiset velvollisuudet

Rekisterinpitäjä määrittelee henkilötietojen käsittelyn tarkoituksen ja keinot eli on se osapuoli jonka intressissä tietojen käsittely tapahtuu. Rekisterinpitäjä kantaa vastuun rekisteristä ja on korvausvastuussa vahingoista ja seuraamuksista mikäli henkilötietojen käsittelyssä on puutteita. Uudistus tiukentaa rekisterinpitäjän vaatimuksia ja velvollisuuksia. Uutta on esimerkiksi osoitusvelvollisuus (Artikla 5) joka tarkoittaa, että rekisterinpitäjän on pystyttävä laatimiensa dokumenttien

avulla osoittamaan viranomaisille että se on valmistautunut rekisterin pitoon, tuntee riskit, on tehnyt tarvittavat toimenpiteet tietosuojan toteutumiseksi ja noudattaa olemassa olevia tietoturvasäädöksiä. Osoitusvelvollisuutta voi toteuttaa myös erilaisilla sertifikaateilla tai alakohtaisilla käytännesäänöillä. Yleisten säädösten lisäksi on huomioitava myös toimialakohtaiset lait ja vaatimukset joita löytyy useilta eri aloilta.

Tietosuoja-asetuksessa on säädetty sisäänrakennetusta ja oletusarvoisesta tietosuojasta (Artikla 25) joka tarkoittaa sitä, että tietosuojaperiaatteet ja -vaatimukset tulisi ottaa huomioon jo hyvin aikaisessa vaiheessa henkilötietoja käsitelevää rekisteriä suunnitellessa. Tietosuojan tulisikin aina olla etukäteen harkittu, olennainen osa organisaatioiden toimintaa eikä vasta jälkeenpäin toteutettu korjaustoimenpide.

4.4.1 Käsittelijän velvollisuudet

Asetuksen 28 artikla määrää henkilötietojen käsittelijöiden toiminnasta. Heidän tulee osaltaan pitää huolta että rekisterinpitäjälle säädetty vastuu ja velvollisuudet toteutuvat. Käsittelijä tarvitsee henkilötietojen käsittelyyn kirjallisen luvan ja kirjallisen ohjeistuksen rekisterinpitäjältä. Henkilötietojen käsittelijä voi olla luonnollisen henkilön lisäksi oikeushenkilö, viranomainen, muu virasto tai elin joka käsittelee henkilötietoja rekisterinpitäjän puolesta. Useimmilla yrityksillä yrityksen ulkopuolisia henkilötietojen käsittelijöitä ovat esimerkiksi palkanlaskijat ja kirjanpitäjät. Henkilötietojen käsittelijä on siis se osapuoli joka tosiasiallisesti käsittelee henkilötietoja rekisterinpitäjän lukuun. (Tietosuoja-asetus 679/2016, Artikla 28)

Rekisterinpitäjän ja käsittelijän välillä tulee olla kirjallinen sopimus jossa oikeudet ja velvollisuudet on yksilöity. Henkilötietojen käsittelyä ei saa aloittaa ennen sopimuksen tekoa. Työpaikoilla toteutus on yksinkertainen määrittelemällä työntekijöiden työtehtävät ja vastuut. Mikäli yrityksen pitämää henkilötietorekisteriä käsittelee yrityksen ulkopuolinen taho, on sopimuksen sisältöön paneuduttava huolella. Tietosuoja-asetuksen artikla 28 määrää tarkemmin myös solmittavan sopimuksen sisällöstä esimerkiksi

salassapitovelvollisuuden noudattamisesta, sopimuksen kestosta, henkilötietojen poistamisesta sopimuksen päättyessä ja niin edelleen. Henkilötietojen käsittelijä, henkilö tai yritys, tekee siis aina töitä rekisterinpitäjän lukuun ja on vastuussa siitä että toimii ainoastaan annettujen ohjeiden ja määräysten mukaan. Tietoja ei saa käsitellä mihinkään muuhun tarkoitukseen vaikka käsittelijällä olisikin jatkuva pääsy tietoihin. (Tietosuoja-asetus 679/2016, Artikla 28)

4.5 Tietosuojavastaava

Tietosuoja-asetuksen 37 artikla määrää tietosuojavastaavasta. Aikaisemmin tietosuojavastaavan nimittäminen on ollut pakollista sosiaali- ja terveydenhuoltoalalla, apteekeilla ja Kelalla (Andreasson ym., 2013, 16). Nyt laki edellyttää tietosuojavastaavan nimittämistä sekä rekisterinpitäjän että henkilötietojen käsittelijän kohdalla mikäli yksikin seuraavista ehdoista täyttyy:

- tietoja käsittelee jokin muu viranomainen tai julkishallinnon elin kuin tuomioistuin

- rekisterinpitäjän tai käsittelijän päätehtävät muodostuvat toimista, jotka edellyttävät rekisteröityjen jatkuvaa seurantaa laajassa mittakaavassa tai

- päätehtävät koostuvat erityisten henkilötietoryhmien käsittelystä joita ovat mm. rikostuomioita koskevat tiedot

Tietosuojavastaavan nimittäminen koskee siis todella monta yritystä ja julkista toimijaa Suomessakin. Isoissa konserneissa tulee myös huomioida että tietosuojavastaavia voidaan nimittää useampia, mikäli yksi henkilö ei riitä olemaan koko konsernin tavoitettavissa. Tietosuojavastaavan täytyy olla alan ammattilainen ja hänellä tulee olla riittävä asiantuntemus alasta. Tehtävä voidaan myös ulkoistaa. Sekä rekisterinpitäjän että henkilötietojen käsittelijän tulee julkisesti ilmoittaa tietosuojavastaavan yhteystiedot ja ilmoittaa ne myös tietosuojavaltuutetun toimistoon. Tietosuojauudistus tuo siis mukanaan myös suurehkot menot varsinkin pienemmille yrityksille. Todennäköisesti jo pelkkä henkilötietojen käsittelyn arviointi vaatii ulkopuolisen asiantuntijan palveluita. Jos tämän lisäksi joudutaan vielä palkkaamaan tietosuojavaltuutettu tai ostamaan

nämä palvelut säännöllisesti, ovat lakimuutoksen tuomat lisäkulut yritykselle jo huomattavat.

Tietosuojavastaavan tulee hoitaa tehtävänsä riippumattomasti ja lain vaatimusten mukaan. Hän raportoi suoraan ylimmälle johdolle jonka vastuulla lain noudattaminen viime kädessä on. Asetuksen mukaan rekisteröidyt voivat ottaa yhteyttä suoraan tietosuojavastaavaan kaikissa asioissa jotka liittyvät heidän tietojensa käsittelyyn tai niihin liittyviin oikeuksiin. Artikla 39 määrittelee tietosuojavastaavan tehtävät joita on oltava vähintään:

a) neuvontavelvollisuus rekisterinpitäjiä ja henkilötietojen käsittelijöitä sekä yksittäisiä rekisteritietoja käsitteleviä työntekijöitä kohtaan

b) velvollisuus seurata tietosuoja-asetuksen sekä muun sovellettavan lainsäädännön toteuttamista

c) antaa neuvoja vaikutuksenarvioinnista ja valvoa sen toteutumista

d) yhteistyön tekeminen valvontaviranomaisten kanssa

e) olla valvontaviranomaisten yhteyshenkilönä mm. ennakkokuulemisia ja muita tehtäviä varten

Tietosuojavastaavaa ei saa erottaa tehtävien hoitamisen vuoksi eikä häntä saa myöskään rangaista hänen hoitaessaan lakisääteisiä velvoitteita. Suunnitellessa yrityksen tietosuojaa tulisi tietosuojavastaavan lisäksi suunnitteluun osallistua henkilöitä jokaiselta osastolta. Vaikka vastuu valvonnasta olisi yhden ihmisen työ, on valvonnan jokapäiväinen toteuttaminen kuitenkin koko organisaation yhteinen tehtävä. Kaikkia henkilötietorekistereiden parissa työskenteleviä tuleekin kouluttaa ja tiedottaa jotta kukaan ei rikkoisi lakia ainakaan tietämättömyyttään.

4.6 Valvontaviranomainen

Suomessa tietosuoja-asetuksen noudattamista valvoo Tietosuojavaltuutetun toimisto. Tietosuojavaltuutettuna toimii tällä hetkellä Reijo Aarnio. Tietosuojavaltuutetun toimenkuvan määrittelee henkilötietolaki sekä laki

tietosuojalautakunnasta ja tietosuojavaltuutetusta (389/1994). Tietosuojavaltuutetun ensisijainen tehtävä on ohjeistaa rekisterinpitäjiä ennakkoon rekisterinpidon lainmukaisuuteen liittyvissä kysymyksissä, kehittää hyvää tietojenkäsittelytapaa sekä ehkäistä tietosuojaloukkausten tapahtumista. Tietosuojavaltuutettu vastaa myös aihealueen kysymyksiin ja tekee kannanottoja. Lainvastaiset tapaukset hän voi ohjata tietosuojalautakunnan käsiteltäviksi. Tietosuojavaltuutettu voi määrätä esimerkiksi henkilötietorekisterin lopetettavaksi mikäli rekisterinpitäjä toimii määräysten vastaisesti. (Tietosuojavaltuutetun toimisto, 2014.)

Uusi asetus (artikla 33) määrää rekisterinpitäjän velvollisuudeksi tehdä tietoturvaloukkauksista ilmoituksen tietosuojavaltuutetulle 72 tunnin sisällä tapahtuneesta. Kaikki tietoturvaloukkaukset sekä niiden korjaavat toimet on myös dokumentoitava jotta viranomaiset voivat tarvittaessa todentaa tämän asetuksen artiklan 33 toteutumisen.

Toisen uutena pykälänä tietosuoja-asetus tuo valvovalle viranomaiselle oikeuden määrätä rekisterinpitäjälle ja myös henkilötietojen käsittelijälle sakkoja tai hallinnollisia seuraamuksia asetuksen velvoitteiden noudattamatta jättämisestä. Artiklassa 83 säädetään sakkojen määrästä. Sakot on jaettu rikkomuksesta riippuen kolmeen eri luokkaan. Korkeintaan sakko voi olla jopa 20 miljoonaa euroa tai 4% yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta. Sakkojen sijasta voidaan myös määrätä muita sanktioita kuten henkilötietojen käsittelyn kieltäminen siihen saakka kunnes virheet on korjattu. Tämänhetkinen henkilötietolaki antaa tietosuojavaltuutetulle mahdollisuuden rajoittaa tai kieltää rekisterinpitäjää käyttämättä rekisteriä jos hän on toiminut lain vastaisesti. Tietosuojavaltuutettu voi myös asettaa uhkasakon määräysten tehostamiseksi.

5 UUDEN TIETOSUOJALAIN TOTEUTTAMINEN REKISTERÖIDYN NÄKÖKULMASTA

Tietosuoja-asetuksessa korostetaan rekisterinpitäjiltä selkeää ja ymmärrettävää kieltä. Rekisterinpitäjän täytyy huolehtia siitä että tarvittava tieto siitä, mitä tietoja henkilöistä rekisteröidään ja mihin niitä käytetään on helposti saatavilla. Toiminnan läpinäkyvyydellä ja avoimuudella tavoitellaan myös asiakkaiden luottamusta. (Tietosuoja-asetus 679/2016, resitaali 39)

Jos henkilötietoja on poistetaan, oikaistaan tai rekisteröity on pyytänyt niiden käsittely rajoittamista, on rekisterinpitäjän ilmoitettava näistä toimenpiteistä myös mahdollisille kolmansille osapuolille joille tietoja on luovutettu. Tietojen vastaanottajat on myös ilmoitettava rekisteröidylle jos hän haluaa ne tietoonsa saada. (Tietosuoja-asetus 679/2016, artikla 19) Lakiuudistus tuo siis mukanaan monelle yritykselle myös paljon kehitettävää yhteistyökumppaneiden ja sidosryhmien kanssa.

5.1 Rekisteröidyn oikeudet

Uudessa tietosuoja-asetuksessa rekisteröidyn oikeuksia on tarkennettu ja niiden tärkeyttä korostetaan. Pääpiirteittäin oikeudet ovat samoja kuin henkilötietolaissakin, mutta uutta on esimerkiksi rekisteröidyn oikeus siirtää henkilötietonsa järjestelmästä toiseen. (Tietosuoja-asetus 679/2016, artikla 20) Rekisterin pitäjälle asiakkaiden joukkotiedonsiirrot voisivat tuoda ongelmia lähinnä siitä syystä että tiedonsiirtoa ei ole automatisoitu ja se sitoo ajan lisäksi työvoimaa. Todennäköistä kuitenkin on, että tiedonsiirrot järjestelmästä toiseen ovat ainakin toistaiseksi vielä yksittäistapauksia.

Asetuksessa on tarkasti selvitetty mitkä ovat rekisterinpitäjän velvollisuuksien ohella rekisteröidyn oikeudet. Rekisteröidylle ei kuitenkaan ole kirjattu asetukseen yhtään velvollisuutta. Miksi rekisteröidylle ei ole siirretty enemmän vastuuta esimerkiksi yhteystietojensa pitämisestä ajan tasalla? On aina rekisterinpitäjän velvollisuus huolehtia että rekisterissä ei käsitellä vanhentunutta tai virheellistä tietoa (täsmällisyysvaatimus). Osa tiedoista, kuten esimerkiksi

puhelinnumero voi kuitenkin olla vaikeaa pitää ajan tasalla ilman rekisteröidyn ilmoitusta muuttuneesta yhteystiedosta.

Rekisteröityä tulee informoida tietojen käsittelystä etukäteen. Henkilötietolain 10§ kertoo rekisterinpitäjän velvollisuudesta ylläpitää rekisteriselostetta joka tulee olla jokaisen saatavilla. Nykyään rekisteriseloste löytyy lähes jokaisen yrityksen verkkosivulta. Uudessa tietosuoja-asetuksessa ei ole sananmukaista mainintaa rekisteriselosteesta, mutta asetuksen 13 artikla esittää tiedot jotka tulee toimittaa kun henkilötietoja kerätään rekisteröidyltä. Käytännössä nämä tiedot esitetään rekisteriselosteessa. Artiklassa korostetaan että tietojen tulee olla helposti saatavissa olevassa muodossa. Tiedot voivat olla paperin lisäksi esimerkiksi PDF-tiedostona jolloin ne on helppo toimittaa sähköisesti. Sen lisäksi niiden tulee olla selkeästi ja ymmärrettävästi kirjoitettu, varsinkin silloin kun kyseessä on lapsille toimitettavista tiedoista. Monilla yrityksillä olisi vielä kehitettävää ymmärrettävien ehtojen toimitettavien tietojen kanssa.

Rekisteröidylle toimitettavat tiedot ennen henkilötietojen käsittelyä ovat rekisterinpitäjän ja mahdollisen tietosuojavastaavan yhteystiedot, henkilötietojen käsittelyn tarkoitus ja oikeusperuste, henkilötietojen vastaanottajat, tieto siitä jos henkilötietoja aiotaan siirtää kolmanteen maahan tai kansainväliselle järjestölle. Läpinäkyvän ja asianmukaisen kohtelun varmistamiseksi on lisäksi ilmoitettava seuraavaa: henkilötietojen säilytysaika, rekisteröidyn oikeudet, oikeus peruuttaa suostumus tietojen antamisesta, oikeus tehdä viranomaisvalitus, tieto siitä onko henkilötietojen toimittaminen vaatimuksena esimerkiksi sopimuksen tekemiseen ja tieto siitä mitä tapahtuu jos rekisteröitävä ei anna tietojaan. Lisäksi rekisteröitävälle tulee toimittaa tiedot automaattisesta päätöksenteosta, sen merkittävyydestä ja sen seurauksista rekisteröidylle. Myös tietojen mahdollisesta jatkokäsittelystä on aina ilmoitettava rekisteröidylle ennen toimenpiteiden aloittamista. (Tietosuoja-asetus 679/2016, artikla 30)

Joissain tapauksissa tietoja rekisteröidystä saatetaan kerätään myös jostain muualta kuin rekisteröidyltä itseltään. Ensimmäisenä tästä toimintatavasta tulee mieleen puhelinmyynti tai mainostamiseen tarkoitettu sähköposti. Harvoin asiakas on antanut yhteystietojaan puhelinmyyjälle, mutta yhteystietojen kerääminen

esimerkiksi julkisesta puhelinluettelosta on laillista. Koskaan en ole kuullut että puhelinmyyjä kertoisi mistä on yhteystietonsa saanut vaikka asetuksen mukaan hänen näin kuuluisi heti ensimmäisen yhteydenoton alussa tehdä. (Tietosuoja-asetus 679/2016, resitaali 61)

Siinä tapauksessa että tiedot on kerätty muualta kuin rekisteröidyltä itseltään, on hänelle ilmoitettava edellisessä kappaleessa mainittujen tietojen lisäksi vielä tiedot seuraavista asioista:

- kerätyt henkilötietoryhmät eli millaisia tietoja rekisteröidystä on kerätty

- rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut eli on annettava informaatio siitä miksi tietojen rekisteröinti on tarpeellista rekisterinpitäjän tai kolmannen osapuolen etujen toteuttamiseksi

- mistä henkilötiedot on saatu ja erikseen on vielä ilmoitettava jos ne on saatu yleisesti saatavilla olevista lähteistä eli esimerkiksi julkisesta puhelinluettelosta (Tietosuoja-asetus 679/2016, artikla 14)

5.1.1 Oikeus saada pääsy tietoihin

Rekisteröidyllä on milloin tahansa oikeus saada pääsy aikaisemmin mainittuihin tietoihin ja tarkistaa hänestä tallennetut tiedot. Henkilötietolain tarkastusoikeuteen nähden tietosuoja-asetuksessa säädetään hieman tarkemmin rekisteröidyn oikeudesta saada pääsy omiin tietoihinsa. Asetuksen artiklan 15 mukaan rekisteröidyllä on oikeus saada kopio niistä tiedoista joita hänestä on tallennettu. Pyynnön esittämiselle ei ole määrämuotoa. (Tietosuoja-asetus 679/2016, artikla 15x)

Rekisterinpitäjän tulee luonnollisesti varmistaa rekisteröidyn henkilöllisyys silloin kun hän haluaa tarkistaa tietojaan, muuttaa niitä tai saada ne siirretyksi johonkin toiseen järjestelmään. Rekisteröidyn tulisi saada vastaus edellä mainittuja pyyntöjä koskien kuukauden sisällä pyynnön esittämisestä. Tämä katsotaan kohtuulliseksi ajaksi. Tarvittaessa aikaa voidaan pidentää kahdella kuukaudella mikäli esitetty pyyntö on erittäin monimutkainen tai pyyntöjä on esitetty monta.

Selvitys tiedoista tulisi ensisijaisesti toimittaa sähköisesti ja maksutta. (Tietosuoja-asetus 679/2016, artikla 12)

5.1.2 Tietojen oikaiseminen ja niiden poistaminen

Artiklan 16. mukaan jokaisella henkilötietorekisteriin merkityllä henkilöllä häntä koskevan tiedon saamisen lisäksi oikeus pyytää rekisterinpitäjää korjaamaan häntä koskevat epätarkat tai virheelliset tiedot. Yleisimmin oikaistavia tietoja ovat hyvin todennäköisesti yhteystiedot. Rekisteröidyllä on aina myös oikeus täydentää puuttuvia tietoja toimittamalla rekisterinpitäjälle tarvittavat lisätiedot. (Tietosuoja-asetus 679/2016, artikla 16)

Rekisteröidyn henkilön oikeus hänestä tallennettujen tietojen poistamiseen eli puhutaan henkilön "oikeudesta tulla unohdetuksi". Oikeus pyytää tietojen poistamista on kuulunut jo myös henkilötietolain piiriin, vaikka sitä ei ole erikseen laissa otsikoitu. Rekisteröidyllä on oikeus vaatia tietojensa poistamista, mikäli tietoja ei enää tarvita siihen tarkoitukseen mihin niitä on kerätty. Rekisteröity voi myös peruuttaa tietojen käsittelyyn antamansa suostumuksen tai vastustaa tietojen käsittelyä. Asetuksessa mainitaan erityisesti myös lapset jotka alaikäisinä ovat antaneet tietonsa johonkin palveluun. He eivät ehkä ole täysin ymmärtäneet mihin tietoja on kerätty tai mihin niitä on käytetty. Tästä syystä myös heillä on oikeus tulla unohdetuksi lapsina, mutta myös myöhemmin aikuisiässä mikäli he niin toivovat (Tietosuoja-asetus 679/2016, resitaali 65).

Asetuksessa on myös mainittu muutama poikkeus jonka nojalla tietoja ei tarvitse poistaa vaikka rekisteröity sitä vaatisi. Tällaisia poikkeuksia voivat esimerkiksi olla tietojen säilyttäminen oikeudellisten vaatimusten laatimista tai oikeudenkäyntiä varten. Tietoja voidaan poistopyynnöstä huolimatta säilyttää myös kansanterveydellisistä syistä ja ne voidaan joissain tapauksissa perustellusti säilyttää myös historiallista tai tilastollista tutkimusta varten. Tiedot on myös poistettava mikäli niitä on käytetty lainvastaisesti tai muuten sopimattomalla tavalla. (Tietosuoja-asetus 679/2016, artikla 17)

Jos henkilötietoja on luovutettu eteenpäin, tulee rekisterinpitäjän viipymättä ilmoittaa poistopyyntö eteenpäin näille tahoille. Henkilötiedot tulee siten pyrkiä poistamaan myös kolmansilta osapuolilta. Mikäli tiedot ovat julkisia, tulee ne pyrkiä poistamaan myös kaikista julkisista lähteistä. (Tietosuoja-asetus 679/2016, artikla 17) Tämä saattaa kuitenkin olla nyky-yhteiskunnassa haastavaa ellei jopa mahdotonta ainakin julkisten tietojen kohdalla. Vaikka tiedot poistettaisiin, on joku jo saattanut kopioida tiedon ja ladata sen edelleen jollekin toiselle verkkosivulle. Jokaisen olisikin syytä pitää mielessä olettamus jonka mukaan kaikki mitä verkkoon ladataan jää sinne jossain muodossa vaikka tieto myöhemmin poistettaisiin.

Tästä hyvänä esimerkkinä Google joka on ruvennut poistamaan tiettyjä hakutuloksia palvelustaan. Jokainen pyyntö käsitellään erikseen ja Google onkin tietosuojaselosteessaan ilmoittanut että ei kuitenkaan poista pyynnöstä esimerkiksi syntymäaikoja, puhelinnumeroita tai osoitteita, vaikka ne ovat keskeisiä henkilörekisterin osia ja yleisimmin käytössä olevia henkilötietoja (Google, 2017). Verkkoon joskus päässyt tieto siis saattaa jäädä sinne pysyvästi vaikka se pyydettäisiin poistamaan.

Euroopan unionin tuomioistuin on toukokuussa vuonna 2014 antanut ennakkopäätökset jonka mukaan Googlen oli poistettava espanjalaismiehen tiedot hakukoneestaan. Tiedot johtivat paikallislehden julkaisemiin tietoihin joissa käsiteltiin mieheltä pakkohuutokaupattua taloa. Mies katsoi että vanhentunut tieto vahingoitti häntä edelleen koska hänen nimensä googlaamalla päätyi hakutuloksista aina kyseisiin tietoihin. Unionin tuomioistuin katsoi että Google rinnastetaan rekisterinpitäjään jolloin sen tuli rekisteröidyn pyynnöstä poistaa häntä koskeva vanhentunut tieto hakutoiminnoistaan. Tiedon julkaiseminen alkuperäisellä sivulla lehdessä oli kuitenkin julkista ja laillista joten miehen tiedot saattoi edelleen löytää netistä. (Unionin tuomioistuin, 2014)

Tässä tapauksessa Google määrättiin poistamaan tiedot hakukonetuloksistaan. Huhutaan kuitenkin edelleen myös siitä, että käyttämällä muiden kuin EU-maiden hakutoimintoa, on poistetut tiedot löydettävissä verkosta edelleen. Ei siis riitä että

tiedot poistetaan vaan oman maan tai alueen hakukonetoiminnoista jos niihin edelleen pääsee käsiksi muualta päin maailmaa. (Virtanen, 2014, 1)

5.1.3 Käsittelyn rajoittaminen ja rekisterinpitäjän ilmoitusvelvollisuus

Rekisteröidyn oikeus henkilötietojensa käsittelyn rajoittamiseen on määritelty tietosuoja-asetuksen artiklassa 18. Henkilö voi rajoittaa tietojensa käsittelyä muutamassa tapauksessa jos tietojen käsittelyssä on epäselvyyttä tai erimielisyyttä. Jos rekisteröity kiistää hänestä tallennettujen tietojen paikkansapitävyyden voi hän kieltää rekisterinpitäjää käsittelemästä tietoja ennen kuin tiedot ovat jälleen ajan tasalla. Tällaisessa tapauksessa rekisterinpitäjä on velvollinen selvittämään tietojen paikkansapitävyyden ja tarvittaessa oikaisemaan väärän tiedon. (Tietosuoja-asetus 679/2016, artikla 18)

Henkilötietojen käsittely voi olla myös lainvastaista, mutta joskus henkilö ei vaadi tietojaan poistettavaksi vaan sen sijaan vaatii että niiden käsittelyä rajoitetaan. Näin menettelevä rekisteröity toimii mielestäni loogisesti halutessaan säilyttää tiedot rekisterissä poistamisen sijaan jotta voi osoittaa niiden väärinkäytön myöhemmin. Rajoitusoikeus pätee myös siinä tapauksessa että rekisterinpitäjä muutoin poistaisi tiedot tarpeettomina, mutta rekisteröity itse tarvitsee niitä oikeudellisiin tarkoituksiin. (Tietosuoja-asetus 679/2016, artikla 18)

Joskus henkilötietojen rekisteröinti voi tapahtua siitä syystä että rekisterinpitäjä on voinut täyttää jonkin yleistä etua vaativan tehtävän tai käyttää hänelle kuuluvaa julkista valtaa. Kun rekisterinpitäjä vetoaa henkilötietojen käsittelyn tapahtuneen rekisterinpitäjän tai kolmannen osapuolen oikeutetun edun toteuttamiseksi, mutta rekisteröity vastustaa tietojen käsittelyä, voidaan tietojen käsittelyä pitää niin sanotusta jäissä sen aikaa kun odotetaan ratkaisua siitä onko rekisterinpitäjä vai rekisteröity oikeassa (Tietosuoja-asetus 679/2016, artikla 18). Ennen kuin henkilötietojen käsittelyä yllä mainituissa tapauksissa niiden käsittelyn rajoittamisen jälkeen jatketaan, on asiasta aina tehtävä ilmoitus rekisteröidylle. Rekisterinpitäjä on myös velvollinen ilmoittamaan rekisteröidyn vaatimuksista

niille kolmansille osapuolille joille tietoja on luovutettu. Ilmoitusvelvollisuus koskee pyyntöjä tietojen rajoittamisesta, poistamisesta tai niiden oikaisusta. (Tietosuoja-asetus 679/2016, artikla 19)

5.1.4 Tietojen siirto järjestelmästä toiseen

Artikla 20 saattaa tuottaa rekisterinpitäjille hieman päänvaivaa. Aikaisemmin rekisterinpitäjä on pyrkinyt salaamaan ja suojaamaan rekisteröidyn tietoja ulkopuolisilta ja varsinkin kilpailijoilta parhaansa mukaan. Nyt rekisteröidyn oikeuksiin on lisätty oikeus siirtää tiedot järjestelmästä toiseen. Oikeuden toteuttamismahdollisuus edellyttää että henkilötietojen käsittely perustuu suostumukseen tai sopimukseen. Edellytyksenä myös on että henkilötietojen käsittely suoritetaan automaattisesti. Tämän oikeuden toteuttamisesta ei saa aiheutua haittaa muiden oikeuksiin tai vapauksiin. Tietojensiirto-oikeutta ei myöskään tarvitse toteuttaa yleistä etua koskevan tehtävän suorittamisessa tai julkisen vallan käyttämisessä. (Tietosuoja-asetus 679/2016, artikla 20)

Tiedot voidaan käytännössä toimittaa rekisteröidylle itselleen tai suoraan rekisteröidyn osoittamalle toimijalle mikäli se on tietoteknisesti mahdollista. Aina samankaan alan yrityksillä ei kuitenkaan ole käytössä samanlaisia järjestelmiä joten käytännön toteutus jää nähtäväksi. Rekisterinpitäjän tulisi artiklan mukaan kuitenkin toteuttaa tietojen toimittaminen koneellisesti luettavassa muodossa. Näin ollen tiedot voidaan esimerkiksi ladata muistitikulle tai vaikka vielä nykyaikaisemmin pilvipalveluun josta ne voidaan edelleen siirtää uuteen osoitteeseen.

5.1.5 Vastustamisoikeus ja profilointi

Mikäli rekisteröidyllä on erityiseen henkilökohtaiseen tilanteeseen liittyvä peruste, on hänellä oikeus vastustaa henkilötietojensa käsittelyä silloin kun niiden käsittelyn peruste on yleistä etua koskevan tehtävän suorittaminen tai silloin kun henkilötietojen käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutetun edun toteuttamiseksi. Vastustusoikeus ei kuitenkaan koske sellaisia

julkisen sektorin rekistereitä joita ylläpidetään lain perusteella. (Tietosuoja-asetus 679/2016, artikla 21)

Vastustamisen jälkeen rekisterinpitäjän on kiellettyä käsitellä niitä henkilötietoja jotka kuuluvat kyseessä olevalle rekisteröidylle. Tietoja saa käsitellä siinä tapauksessa että rekisterinpitäjä pystyy osoittamaan pätevän syyn joka syrjäyttää rekisteröidyn oikeudet. Tietoja saa käsitellä myös jos se on tarpeen oikeudellisen vaatimuksen laatimisessa, esittämisessä tai puolustamisessa. Sama vastustamisoikeus pätee myös historiallisin, tilastollisin tai tieteellisin syin tehtyjä tutkimuksia kohtaan, ellei voida osoittaa pätevää syytä sille miksi tietojen käsittely on tarpeen yleistä etua koskevan tehtävän hoitamiseksi. (Tietosuoja-asetus 679/2016, artikla 21)

Silloin kun henkilötietoja käytetään suoramarkkinointiin tai markkinoinnin profilointiin, on rekisterinpitäjän lopetettava näiden tietojen käyttö heti sen jälkeen kun rekisteröity on tietojen käyttöä vastustanut. Rekisteröidylle on selkeästi kerrottava että hänellä on oikeus vastustaa tietojensa käyttöä. Rekisteröidyn henkilön oikeuksiin kuuluu myös se, että hän voi vastustaa automaattisesti tehtyjä päätöksiä. (Tietosuoja-asetus 679/2016, artikla 22) Tällaisia voivat olla esimerkiksi automatisoidut luottopäätökset. Mikäli henkilö vastustaisi automatisoitua päätöstä, on hänellä oikeus vaatia asia uudelleen käsitellyksi manuaalisessa päätöksenteossa tai riitauttaa saamansa päätös. Se ei kuitenkaan tarkoita että lopputulos olisi sen erilaisempi, vaikka ihminen tekisi päätöksen koneen sijaan.

Myös henkilöä koskevan profiloinnin kieltäminen on uudessa asetuksessa mahdollista. Niin profilointia kuin automaattista päätöksentekoa saa kuitenkin harjoittaa mikäli henkilö on antanut siihen suostumuksensa ja jos ne ovat välttämättömiä esimerkiksi rekisteröidyn ja rekisterinpitäjän välisen sopimuksen täyttämiseksi. (Tietosuoja-asetus 679/2016, artikla 22) Käytännössä siis esimerkiksi verkossa tehtävän luottokorttihakemuksen automatisoidun luottopäätöksen tai siinä samassa tehtävän profiloinnin vastustaminen voi olla aika hankalaa jos kyseessä olevan luottokortin haluaa itselleen saada.

5.1.6 Oikeus saada tieto tietoturvaloukkauksista

Sen lisäksi että tietoturvaloukkauksista on ilmoitettava tietotosuojavaltuutetulle, tulee siitä jatkossa aina ilmoittaa myös rekisteröidylle itselleen. Ilmoitus on tehtävä ilman aiheetonta viivytystä. Sen lisäksi että ilmoitetaan mitä on tapahtunut ja mitä tapahtuma tarkoittaa henkilön kannalta jonka tietoturvaa on loukattu tulee ilmoittaa myös tietosuojavastaavan yhteystiedot, seuraukset, toteutetut toimenpiteet ja mahdolliset jatkotoimenpiteet. (Tietosuoja-asetus 679/2016, artikla 34)

Ilmoituksen tekeminen rekisteröidylle ei ole tarpeellista jos tietoturvaloukkauksen kohteeksi joutuneet tiedot on salattu tai saatettu jotenkin muuten sellaiseen muotoon että niihin käsiksi pääsevä henkilö ei niitä ymmärrä. Ilmoituksen tekeminen on tarpeetonta myös jos rekisterinpitäjä on jo toteuttanut sellaisia jatkotoimenpiteitä joilla rekisteröityneen oikeuksiin ja vapauksiin kohdistunut korkea riski ei todennäköisesti enää toteudu. Tietoturvaloukkauksesta on tehtävä julkinen tai muu yhtä tehokas tiedonanto mikäli rekisteröidylle ilmoittaminen muuten vaatisi kohtuutonta vaivaa. Mikäli rekisterinpitäjä ei ole ilmoittanut tapahtuneesta rekisteröidylle ennen kuin hän tekee ilmoituksen tietosuojavaltuutetulle, voi valtuutettu vaatia tekemään ilmoituksen myös rekisteröidylle tai arvioida onko sen tekeminen tarpeellista. (Tietosuoja-asetus 679/2016, resitaali 86-88)

Tällä hetkellä teleyritykset ovat jo velvollisia raportoimaan Viestintävirastolle kaikista henkilötietoihin ja muihin palveluihinsa kohdistuvista tietoturvaloukkauksista tai uhista. Jatkossa ilmoitusvelvollisuus tulee siis koskemaan myös muita organisaatioita. Viestintäviraston julkaiseman seurannan mukaan teleyritysten raportoimien tietoturvauhkien määrä on vuoden 2013 jälkeen ollut laskussa. Henkilötietojen loukkaus tai asiakastietojen hallinnan virhe oli vuonna 2015 noin 40% tapauksista. Vuonna 2016 myös tämä määrä oli laskussa ja oli enää vain noin 20% kaikista tapauksista. Tästä voisi ehkä vetää johtopäätöksiä että tietosuoja on parantunut vuosien myötä ainakin telealan yrityksissä. (Viestintävirasto, 2017) Todennäköisesti yritykset myös kiinnittävät turvallisuuteen nykypäivänä entistä enemmän huomioita. Yleisellä tasolla luulen

että tietosuojaloukkausten määrä on kuitenkin noussut. Aika ajoin saa lukea esimerkiksi pankkeihin ja sosiaalisen median tileihin kohdistuneista hyökkäyksistä. Usein yritykset ilmoittavat asiakkailleen hyökkäyksistä julkisesta ja pyytävät asiakkaita esimerkiksi vaihtamaan sisäänkirjautumistietonsa ja salasanansa. Myös sähköpostilla lähetetyt virukset ja huijaukset ovat valitettavasti tätä päivää ja niiden lähettäjän selvittäminen usein mahdotonta.

5.2 Tiedonhaku rekisteröitynä

Internetin aikakaudella tiedonhaku on jo suhteellisen helppoa. Hakukoneita käyttämällä saa helposti selville monia asioita. Lakien tulkitseminen on kuitenkin monelle haastavaa ja omista oikeuksista ei aina olla selvillä. Uudesta tietosuoja-asetuksesta löytyy informaatiota monesta eri lähteestä ja muun muassa Tietosuojavaltuutettu on koonnut sivulleen perustiedot rekisteröityjen oikeuksista.

Rekisteröitynä omien tietojen tarkastaminen on pääsääntöisesti ilmaista kerran vuodessa. Useimmin tehdyistä pyynnöistä on rekisterinpitäjällä oikeus ottaa kohtuullinen, kulut kattava maksu. Mikäli rekisteröity haluaa selvittää hänestä tallennettuja tietoja tai käyttää muita hänelle säädettyjä oikeuksia tulee hänen esittää pyyntönsä ensisijaisesti suoraan rekisterinpitäjälle. Pyynnön voi tehdä vapaamuotoisesti, mutta apuna voi myös käyttää Tietosuojavaltuutetun toimiston verkkosivuilta löytyvää mallilomaketta. Mikäli rekisteröity ei pysty selvittämään asiaansa tai vaatimuksiaan rekisterinpitäjän kanssa, voi hän ottaa yhteyttä tietosuojavaltuutetun toimistoon. (Tietosuojavaltuutetun toimisto, 2014) Mikäli henkilötietojen käsittelyssä saattaa olla kyse rikoksesta, voi rekisteröity pyytää myös poliisia selvittämään asiaa.

Oikeus nähdä rekisteriseloste on pääsääntöisesti rekisterinpitäjän toimipaikassa (Tietosuojavaltuutetun toimisto, 2014). Nykyisin monella yrityksellä on rekisteriseloste nähtävillä myös yrityksen verkkosivuilla. Jos yritys toimii pääsääntöisesti verkossa, myös rekisteriselosteen on tietysti oltava ensisijaisesti nähtävillä verkossa.

Mikäli rekisterinpitäjä kieltäytyy antamasta pyydettyjä tietoja tai korjaamasta niitä, on hänen annettava siitä kirjallinen todistus. Todistuksesta tulee käydä ilmi ne syyt, joiden vuoksi tarkastusoikeus on evätty. Laissa esitetään kuitenkin poikkeuksia tiettyjä tilanteita varten ja eräät rekisterit on jätetty kokonaan tarkastusoikeuden ulkopuolelle. Tällaisia rekistereitä ovat esimerkiksi poliisin epäiltyjen tietojärjestelmä ja ilmiantorekisteri. (Tietosuojavaltuutetun toimisto, 2014)

Tietosuoja-asetuksen ulkopuolelle jäävät suoramarkkinointikiellot tulee myös esittää suoraan rekisterinpitäjälle. On olemassa myös erilaisia vapaaehtoisia rekistereitä joihin suoramarkkinointikiellon voi ilmoittaa. Rekisteristä kiellot ilmoitetaan tällöin suoraan jäsenyrityksille. Tietoja markkinointiin luovuttavat myös esimerkiksi Väestörekisterikeskus ja Trafi joille voi myös erikseen ilmoittaa kiellosta. Toistaiseksi ei ole olemassa vain yhtä paikkaa suoramarkkinointikiellon tekemiselle, vaan rekisteröidyn on itse otettava selvää eri vaihtoehdoista. (Väestörekisterikeskus, 2017)

6 JOHTOPÄÄTÖKSET

Tietosuoja-asetus tuo mukanaan suuria muutoksia. Monilla yrityksillään on edessä tietosuojavastaavan palkkaaminen ja yrityksen tietosuojakäytäntöjen dokumentoiminen. Lakimuutoksen pitäisi kuitenkin helpottaa esimerkiksi kansainvälisesti toimivia yrityksiä, koska säännöt ovat jatkossa samat koko EU-alueella. Useassa maassa toimivien yritysten tarvitsee myös jatkossa olla yhteydessä vain yhteen tietosuojaviranomaiseen eikä erikseen jokaisen maan viranomaiseen. Toivottavasti yritykset alkavat viimeistään nyt tosissaan ottamaan tietosuojan huomioon jokaisessa vaiheessa. Viimeistään asetukset mahdollistamat tuntuvat sanktiot luulisi antavan tähän vauhtia.

Mielestäni monella verkkosivulla olisi vielä parannettavaa erityisesti ehtojen esittämisessä. Henkilötietojen rekisteröinnin käsittelyn perusta tulisi olla palvelun käyttäjälle selvillä jo ennen kuin mitään henkilötietoja kerätään. Selkeä ja ymmärrettävä kieli kulkee kuitenkin valitettavan harvoin käsikädessä palveluehtojen kanssa. On mielestäni vieläkin yleistä että kaikki lakiteksti kirjoitetaan mahdollisimman vaikeaselkoisesti. En tiedä onko tämä kenenkään etu jos kumpikin osapuoli pystyy vetämään ehdoista omat johtopäätöksensä. Verkkosivuilta tilatessani tarkistan esimerkiksi itse aina palautusoikeudet. Mikäli palautustiedot on helppo löytää ja ne on selkeästi ilmaistu, tilaan tuotteen. Jos ostamaani tuotetta ei saa palauttaa ilmaiseksi tai en löydä palautusehtoja verkkosivuilta, jätän tuotteen ostamatta ja siirryn seuraavaan verkkokauppaan. Ongelmia ehtojen esittämisessä verkkosivuilla esiintyy useimmin pienillä yrityksillä. Suurilla yrityksillä tärkeimmät ehdot on usein selkeästi esitetty ja ne on helppo löytää. Vuoropuhelu asiakkaiden kanssa on myös todella tärkeää. Omassa työssäni olen huomannut että parhaimmat oivallukset tulevat usein palvelun käyttäjiltä ja asiakkailta saatua palautetta kannattaa todella arvostaa.

Kuten aikaisemmin todettu, rekisteröidylle ei asetukseen ole kirjattu velvollisuuksia vaan asetus velvoittaa ainoastaan rekisterinpitäjiä. Yritykset voivat omien ehtojensa avulla velvoittaa palveluiden käyttäjiä tietyissä rajoissa. Lait on kuitenkin aina säädetty suojelemaan heikompaa osapuolta ja esimerkiksi

kuluttajansuojalaki (KSL 38/1978) rajoittaa ja antaa ohjeita kohtuuttomien sopimusehtojen varalta. Jos jostain uskoisin uuden asetuksen myötä ongelmia syntyvän niin se on profilointi. Sitä käytetään laajasti markkinoinnissa, koska kohdennettu markkinointi on tehokkaampaa. Ihmisten kulutuskäyttäytymisestä, nettisivujen käytöstä, sosiaalisesta mediasta ja lähes kaikesta muusta mahdollisesta kerätään jatkuvasti tietoa. Voi olla hankalaa kieltää kaikkea itseensä kohdistuvaa profilointia jos ei ole täyttä selvyyttä missä kaikkialla sitä käytetään. Toisaalta taas yritysten on jatkossa saatava nimenomainen suostumus myös profilointiin ja sitä saa tehdä vain mikäli se on välttämätöntä sopimuksen täytäntöönpanoa varten. Suostumuksen saaminenkin voi asettaa omia haasteitaan.

Rekisteröityjen kannalta uusi asetus tuo kuitenkin paljon hyviä parannuksia. Rekisteröityjen oikeuksia on selkeytetty ja ne on kirjattu asetukseen tarkemmin. Vaatimukset yritysten sisäänrakennetusta ja oletusarvoisesta tietosuojasta tuo rekisteröidylle turvaa ihan alusta asti. Rekisteröidyn on mielestäni helppo ymmärtää asetuksesta ne kohdat joissa hänen oikeuksistaan kerrotaan. Omat oikeudet kuten tarkastusoikeus, oikeus tulla unohdetuksi sekä oikeus korjata virheelliset tiedot on helppo sisäistää. Lainkohdat rekisteröityjen oikeuksista ovat mielestäni selkeät. Uskon että yritykset löytävät niihin myös nopeasti toimivat käytännöt mikäli heillä ei jo sellaisia ole. Pyynnöt rekisterinpitäjälle kannattaa aina tehdä kirjallisesti jotta niistä jää todiste. Asetuksessa on määrätty ajat johon mennessä rekisterinpitäjän tulee antaa vastauksensa. Mikäli yhteistyö rekisterinpitäjä kanssa ei toimi, voi rekisteröity olla viimekädessä yhteydessä tietosuojavaltuutettuun.

Kansalaisia todennäköisesti helpottaa yhtenäinen säätely koko EU:n alueella. Jatkossa kaikilla asukkailla samat oikeudet ja yrityksillä velvollisuudet. Myös varhainen puuttuminen tietoturvaloukkauksiin ja niiden ilmoitusvelvollisuus on merkittävä parannus rekisteröidyn kannalta. Hyvin toteutettu tietosuojauudistus lisää kuluttajan luottamusta yrityksiä kohtaan. Mielestäni juuri tämän kaltaiset lakiuudistukset tuovat tunnetta yhtenäisestä EU-alueesta.

LÄHTEET

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2013. Tietosuojavastaavan käsikirja. Helsinki. Tietosanoma Oy.

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2014. Tietosuojavastaavan käsikirja 2. Helsinki. Tietosanoma Oy.

Bergström, E. 2014. Tietoyhteiskuntakaari. Eduskunnan kirjaston julkaisut. Viitattu 09.04.2017 https:// www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/tietoyhteiskuntakaari.aspx

EUR-Lex. 2015. Sähköisen viestinnän sääntelyjärjestelmä. Viitattu 09.04.2017. http://eur-lex.europa.eu/ legal-content/FI/TXT/?uri=LEGISSUM:l24216a

Euroopan Komissio. 2017. Lehdistötiedote. Komissio ehdottaa korkeatasoisen yksityisyydensuojan varmistavia sääntöjä kaikkeen sähköiseen viestintään ja päivittää EU:n toimielimiä koskevia tietosuojasääntöjä. Viitattu 9.4.17. http://europa.eu/rapid/press-release_IP-17-16_fi.htm

Euroopan Parlamentin ja neuvoston asetus 2016/679. Yleinen tietosuoja-asetus. Säädös säädöstietopankki Eur-Lexin sivuilla. Viitattu 09.04.2017. http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&qid=1503916483312&from=EN

Euroopan unioni. Sähköisen viestinnän sääntelyjärjestelmä. 2002. Säädös säädöstietopankki Eur-Lexin sivuilla. Viitattu 09.04.2017. http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=LEGISSUM: l24216a&from=FI

European Comission. 2016. Article 29 Working Party. Viitattu 09.04.2017. http://ec.europa.eu/newsroom/ just/item-detail.cfm?item_id=50083

European Parliament. 2001. Data Protection Guide. Viitattu 26.08.2017. http://www.europarl.europa.eu/pdf/ data_protection/guide_en.pdf

Facebook. 2015. Oikeus- ja vastuulauseke. Viitattu 16.04.2017. https://www.facebook.com/legal/terms

Google. 2017. Verkkohaku ohjeet. Poistokäytännöt. Viitattu 09.04.2017. https://support.google.com/ websearch/answer/2744324

HE 96/1998. Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi. https:// www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_96+1998.pdf

Neuvonen, R. 2014. Yksityisyyden suoja Suomessa. 1.painos. Viro. Kauppakamari.

Pitkänen O., Tiilikka P. & Warma, E. 2013. Henkilötietojen suoja. Helsinki. Talentum Media Oy.

Ruonala, M. 2011. EU-Perusteos. 2. uusittu laitos. Sastamala. Ulkoasiainministeriön eurooppatiedotus.

Saarenpää, Ahti (2012). Henkilö- ja persoonallisuusoikeus. Teoksesta: Oikeusjärjestys osa 1, 288-409. Tammilehto, Timo. Rovaniemi: Bookwell Oy. ISBN 978-952-484-485-7.

Tietosuojavaltuutetun toimisto. 2014. Rekisteröidyn tarkastusoikeus. Viitattu 09.10.2017. http://www.tietosuoja.fi/fi/index/rekisteroidylle/rekisteroidynoikeudet/tarkistusoikeus.html

Tietosuojavaltuutetun toimisto. 2014. Rekisteriseloste. Viitattu 09.10.2017. http://www.tietosuoja.fi/fi/index/useinkysyttya/rekisteriseloste.html

Tietosuojavaltuutetun toimisto. 2014. Tarkastusoikeus. Viitattu 09.10.2017. http://www.tietosuoja.fi/fi/index/rekisteroidylle/rekisteroidynoikeudet/tarkistusoikeus.html

Tietosuojavaltuutetun toimisto. 2012. Tietosuojavaltuutettu vaatii yrityksiä panostamaan tietoturvaan. Lehdistötiedote. Viitattu 25.8.2017. http://tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/2012/10/tietosuojavaltuutettuvaatiiyrityksiapanostamaantietoturvaan.html

Tietosuojavaltuutetun toimisto. 2014. Tietosuojavaltuutetun toimisto; Tietosuojavaltuutetun toimisto on päällikkövirastona toimiva asiantuntijaorganisaatio oikeusministeriön hallinnonalalla. Viitattu 27.08.2017. http://tietosuoja.fi/fi/index/tietosuojavaltuutetuntoimisto.html

Tilastokeskus. 2016. Suomalaiset käyttävät internetiä yhä useammin. http://tilastokeskus.fi/til/sutivi/2016/ sutivi_2016_2016-12-09_tie_001_fi.html?ad=notify Viitattu 08.04.17

Twitter. 2016. Terms Of Service. Viitattu 16.4.2017. https://twitter.com/tos

Unionin tuomioistuin. 2014. Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González. Audiencia Nacionalen esittämä ennakkoratkaisupyyntö. EUR-Lex. http://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1492184359301&uri=CELEX:62012CJ0131

Vanto, J. 2011. Henkilötietolaki käytännössä. 1. painos. Helsinki. WSOYpro Oy.

Viestintävirasto. 2017. Tilasto: Merkittävien tietoturvaloukkausten ja -uhkien määrät ja tyypit. Viitattu 26.08.2017. https://www.viestintavirasto.fi/tilastotjatutkimukset/tilastot/2016/merkittavientietoturvaloukkaustenja-uhkienmaaratjatyypit.html

Virtanen, M. 2014. Oikeus tulla unohdetuksi. Viitattu 15.4.16. https://www.iprinfo.com/verkkolehti/ kaikki_artikkelit/2014/3_2014/fi_FI/oikeus_tulla_unohdetuksi/

Väestörekisterikeskus. 2017. Tietojen luovutuksen kieltäminen. Viitattu 09.10.2017. http://vrk.fi/vaestotietojarjestelma/tietojen-luovutuksen-kieltaminen

WhatsApp. 2016. Terms Of Service. Viitattu 16.04.2017. https://www.whatsapp.com/legal/?l=fi#terms-of-service

39/1889. Rikoslaki. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 08.04.2017. http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

523/1999. Henkilötietolaki. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 08.04.2017. http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

95/46/EY. 2015. Euroopan parlamentin ja neuvoston direktiivi yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta. (Tietosuojadirektiivi). Säädös säädöstietopankki Eur-Lexin sivuilla. Viitattu 08.04.2017. http://eur-lex.europa.eu/legal-content/FI/TXT/?qid= 1492185348258 &uri=CELEX:31995L0046

2000/C 364/01. Euroopan Unionin perusoikeuskirja. 2000. Säädös säädöstietopankki Eur-Lexin sivuilla. Viitattu 08.04.2017. http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:12012P/TXT

2002/58/EY. 2002. Euroopan parlamentin ja neuvoston direktiivi henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla. (Sähköisen viestinnän tietosuojadirektiivi) Säädös säädöstietopankki Eur-Lexin sivuilla. Viitattu 08.04.2017. http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri= CELEX:32002L0058&qid= 1503915055265&from=EN

2007/C 306/01. Lissabonin sopimus. Viitattu 09.04.2017. http://eur-lex.europa.eu/legal-content/ FI/TXT/PDF/ ?uri= OJ:C:2007:306:FULL&from=en

471/1987. Henkilörekisterilaki. Säädös säädöstietopankki Finlexin sivuilla. Viitattu 08.04.2017. http://www.finlex.fi/fi/laki/alkup/1987/19870471